

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 2:22-mj-596

The digital devices as listed in Attachment A that were
obtained from the residence of Patrick SAULTZ at 140
Whitethorne or the vehicle of SAULTZ in Columbus, OH and
held in the custody of the Columbus Division of Police.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):

SEE ATTACHMENT A (incorporated by reference)

located in the Southern District of Ohio, there is now concealed (identify the
person or describe the property to be seized):

SEE ATTACHMENT B (incorporated by reference)

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841, 843, 848	Distribution/Possession with Intent or Conspiracy to Distribute Controlled Substances and Use of Communications Facility in Commission of Such
18 U.S.C. §§ 1591, 1594	Sex Trafficking, Conspiracy to Commit Sex Trafficking
18 U.S.C. §§ 1595, 1957	Money Laundering

The application is based on these facts:


SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

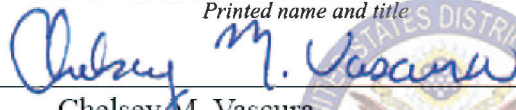
Date: 9/7/2022

City and state: Columbus, Ohio


Applicant's signature

HSI SA Trace Way

Printed name and title


Chelsey M. Vascara
United States Magistrate Judge
Judge's signature

Chelsey M. Vascara, U.S. Magistrate Judge

Printed name and title

- UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO**

Federal investigations involving the illegal possession of firearms and narcotics in conjunction with human trafficking and prostitution, human trafficking, and narcotics trafficking.

3. I have participated in the execution of search warrants and arrests related to the above-referenced offenses. I have seized or assisted in seizing contraband and evidence, including currency, narcotics, firearms, and documentary evidence, which includes electronically stored documents. I have received criminal investigative training, including 26 weeks of intensive training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. This training included instruction on the methods used by criminals to violate the laws of the United States and evade detection by law enforcement. I have had formal and on-the-job training in matters involving human trafficking and narcotics trafficking from instructors, supervisors, and colleagues. I have been personally involved in investigations concerning the possession, manufacture, transportation, distribution, and importation of controlled substances, as well as methods used to finance drug transactions. I am knowledgeable in the enforcement of state and federal laws pertaining to narcotics and dangerous drugs.
4. By virtue of my experience and training, your affiant is familiar with money laundering techniques utilized by individuals involved in illegal activities, such as narcotics and human trafficking. Your affiant knows that it is common for people involved in these types of illegal activities to accumulate large sums of U.S. currency that they seek to launder in order to avoid detection of their illegal activities, and to attempt to freely spend the cash without drawing law enforcement scrutiny. As a result of my training and experience, I am familiar with how drug trafficking organizations illegally traffic, transport, and distribute narcotics and the proceeds derived from the distribution of narcotics. Throughout this affidavit, reference to "investigators" specifically refers to criminal investigators.
5. Based on my training and experience as a law enforcement officer, I also know that members of drug trafficking organizations (DTO) depend on communicating with each other for the purpose of successfully trafficking narcotics. I understand that international and domestic telephone communications are vital to members of a global drug trafficking organization to successfully coordinate and organize the smuggling, transportation, and

distribution of illegal narcotics to the United States. Domestic and international drug traffickers depend on telephone communications to cryptically discuss their illegal activities. International telephone communications allow narcotics traffickers to maintain contact with drug associates, drug suppliers, and drug customers operating in different countries. Cellular telephone texts and other electronic messaging also enable drug trafficking organizations to maintain contact with the associates, drug suppliers, and customers. The telephonic electronic communications are often rapidly followed by telephonic contact with the individual signaling the electronic message. Drug trafficking organizations frequently use cellular electronic messaging features to communicate with associates relating to the logistics of their drug trafficking business. I am also aware that many drug trafficking organizations utilize cellular telephones as an electronic means of communication in an effort to clandestinely communicate without law enforcement interception.

6. Through instruction, training, and participation in investigations, I have become familiar with the manner and methods by which narcotics traffickers and sex traffickers conduct their illegal business and the language and terms that are used to disguise conversations about their narcotics activities. From experience and training, I have learned that drug traffickers believe their conversations are susceptible to interception and rarely overtly discuss their illegal activities. Instead, to conceal the true nature of their illegal activities and to avoid detection by law enforcement, drug traffickers use coded words and phrases to describe narcotics, currency, and locations. Moreover, narcotics traffickers and sex traffickers frequently use telephone communications to further their illegal activities by, among other things, remaining in constant communication with one another, either verbally or via text messaging.
7. I am also aware that drug traffickers and sex trafficking organizations utilize pre-paid telephones with a direct connect (DC) feature that have either no subscriber listed, or a bogus subscriber listed. I am aware that those involved in illegal drug operations often list their telephone and cellular telephones in the names of others or in fictitious names to conceal their identities for illegal purposes, and to thwart law enforcement detection and prosecution. It is likewise essential that such organized groups meet to formulate plans

concerning narcotics or other illegal activities, and to divide their illegal proceeds. I am also aware that drug traffickers and sex traffickers often utilize more than one communication device at one time in order to facilitate their drug trafficking activities. Through my employment as a law enforcement officer, I have gained knowledge in the use of various investigative techniques including the use of judicially-authorized Title III intercepts, physical surveillance, undercover agents, confidential informants, cooperating witnesses, the controlled purchases of illegal narcotics, electronic surveillance, consensually-monitored recordings, investigative interviews, trash pulls, financial investigations, the service of administrative and grand jury subpoenas, and the execution of search and arrest warrants.

PURPOSE OF THE AFFIDAVIT

8. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of a cell-site search warrant; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for a search warrant for the content of numerous digital devices that were seized from the residence of Patrick **SAULTZ** located at 140 Whitethorne Avenue, Columbus, Ohio 43223, and/or **SAULTZ'** black 2019 BMW 750i, bearing temporary Ohio registration O031151, all of which are currently held in the custody of the Columbus Division of Police located at 724 E Woodrow Ave in Columbus, Ohio (hereinafter referred to as the **SUBJECT DEVICES**). I have not omitted any facts that would negate probable cause.
9. The **SUBJECT DEVICES** to be searched are more particularly described in **Attachment A**, for the items specified in **Attachment B**, which items constitute instrumentalities, fruits,

and evidence of violations of A) the distribution and possession with intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); (B) the use of a communications facility in the commission of controlled substances offenses, in violation of Title 21, United States Code, Section 843(b); (C) attempts and conspiracies to commit the aforementioned crimes, in violation of Title 21, United States Code, Section 846; (D) money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957; (E) aiding and abetting the aforementioned crimes, in violation of Title 18, United States Code, Section 2; (F) sex trafficking by means of force, threats, fraud, or coercion, in violation of Title 18, United States Code, Sections 1591(a); and (G) obstruction or conspiracy to commit sex trafficking, in violation of Title 18, United States Code, Section 1591(d) and 1594; (hereinafter collectively referred to as the **TARGET OFFENSES**). I am requesting authority to forensically examine the entirety of the **SUBJECT DEVICES**, wherein the items specified in **Attachment B** may be found, and to seize all items listed in **Attachment B** as instrumentalities, fruits, and evidence of crime.

STATUTORY AUTHORITY

10. As noted above, this investigation concerns alleged violations of the following:

- a. Title 21, United States Code, Section 841 makes it a federal crime for any person to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute or dispense a controlled substance. Subsection (b) of this section makes cocaine, cocaine base, heroin, N-phenyl-N-[1-(2-phenylethyl)-4-piperidinyl] propanamide, commonly referred to as fentanyl, and any of their isomers controlled substances.
- b. Title 21, United States Code, § 846, makes it a crime for any person to attempt or conspire to commit any offense defined in Section 841.
- c. Title 21, United States Code § 843(b) makes it unlawful for any person knowingly or intentionally to use any communication facility in committing or causing or facilitating the commission of any act or acts constituting a felony under any provision of this subchapter or subchapter II of this chapter. Each separate use of a communication facility shall be a separate offense under this subsection. For the purpose of this subsection,

the term “communication facility” means any and all public and private instrumentalities used or useful in the transmission of writing, signs, signals, pictures, or sounds of all kinds and includes mail, telephone, wire, radio, and all other means of communication.

d. Title 18, United States Code § 1956 makes it unlawful to, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conduct or attempt to conduct such a financial transaction which, in fact, involves the proceeds of a that specified unlawful activity and that it is done with the intent to promote the carrying on of specified unlawful activity knowing that the transaction is designed to, in whole or in part, conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of the specified unlawful activity or to avoid a transaction reporting requirement under State or Federal law.

e. Title 18, United States Code § 1957 makes it unlawful to knowingly engage or attempt to engage in a monetary transaction in a criminally derived property of value greater than \$10,000 and is derived from specified unlawful activity.

f. Title 18, United States Code § 2 makes it a crime to aid or abet in any of the aforementioned crimes.

g. Title 18, United States Code § 1591 makes it a federal crime for any person, in or affecting interstate or foreign commerce to recruit, entice, harbor, transport, provide, obtain, advertise, maintain, patronize or solicit, by any means, a person, knowing, or in reckless disregard of the fact that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act. Section 1594 of the same title prohibits attempts or conspiracies to engage in such acts.

h. Pursuant to Title 18, United States Code, Section 1591(e) (3) the term “commercial sex act” is defined as “any sex act, on account of which anything of value is given to or received by any person.”

APPLICABLE DEFINITIONS

11. The term “computer”¹ is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
12. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
13. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
14. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
15. As it is used throughout this affidavit and all attachments hereto, the term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

¹The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

**BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES,
MOBILE APPLICATIONS, AND THE INTERNET**

16. I know from my training and experience that computer hardware, computer software, and electronic files (“objects”) may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
17. Computers, tablets and smart/cellular phones (“digital devices”) are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a “scanner,” which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including “GIF” (Graphic Interchange Format) files, or “JPG/JPEG” (Joint Photographic Experts Group) files.
18. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including “MPG/MPEG” (Moving Pictures Experts Group) files.
19. Digital devices are also capable of sending and receiving messages. Messages can be received or sent on digital devices in a variety of manner, including, but not limited to, e-mail, texting (including “SMS” and “MMS” messaging), and application messaging (including, but not limited to, Facebook Messenger, Snapchat, and WhatsApp).

20. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.
21. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
22. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are

replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

23. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
24. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in **Attachment B**.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

25. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
- A. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in

random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

B. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

26. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

PROBABLE CAUSE

27. In 2021, the Central Ohio Human Trafficking Task Force (COHTTF) initiated an investigation into Cordell **WASHINGTON** aka “Bro” aka “Dub” and Patrick **SAULTZ** aka “White Boy Pat”, who are alleged to be the leaders of a Drug Trafficking Organization (DTO) in Columbus, Ohio. Investigators have since learned this DTO is engaged in a large-scale conspiracy involving narcotics distribution, sex trafficking, fraud, and money laundering. The results of the investigation thus far have indicated that the DTO is bringing in large quantities of fentanyl and cocaine into Columbus, Ohio. These drugs were being sold in and around the Columbus area while simultaneously being used to coerce individuals to engage in sexual

activity for profit, from which the DTO benefits. In beginning their investigation into the sex trafficking portion of this DTO, the COHTTF learned that **SAULTZ** was already under investigation with the DEA along with his co-target Cordell **WASHINGTON** since 2020.

28. Through the ongoing investigation, investigators have identified several individuals associated with this DTO. The associates are engaged in the day-to-day operations of the DTO related to the **TARGET OFFENSES**. Numerous individuals have been identified as being participants of the illicit activity being conducted by this DTO and include, but are not limited to, Patrick **SAULTZ** aka "White Boy Pat", aka "Pat," Cordell **WASHINGTON** aka "DUB", aka Cory, aka "Bro," David **PRICE** aka "DP", and aka "Beast," Tyler **BOURDO**, and **ALLISON** Smith aka "Allie" (herein after collectively referred to as **TARGET SUBJECTS**).
29. In continuing investigation into the illegal activities of this DTO, undercover buys were made, confidential sources were utilized, and physical and electronic surveillance were employed. In addition, numerous interviews were held with individuals related to this DTO. For example, interviews were conducted with Sarah **BURRIS**, who is now deceased due to a drug overdose. Investigators had previously identified **BURRIS** as an individual who had direct knowledge of this DTO from one of the original tips they had received from CPD when they initiated their investigation into the sex trafficking portion of the case. **BURRIS** had also previously disclosed that she was a victim of this DTO's sex trafficking. In summary, during the multiple interviews of **BURRIS**, she advised that **PRICE** was selling drugs and providing women with drugs in exchange for sexual favors. **BURRIS** indicated that the men were using an online website called "Megapersonals" to place escort ads for women to engage in solicitation for prostitution which this investigation corroborated as indicated above. **BURRIS** stated she believed the person who oversees the operation is David **PRICE**. **BURRIS** stated she solicited by posting Escort Ads and "walked the block" but that all the money she made was then spent on **PRICE**'s drugs. **BURRIS** clarified that if she did not spend money at **PRICE**'s trap house, she would "get her ass beat" and that ultimately, the money ended up back with **SAULTZ** because he oversaw everything. **BURRIS** also indicated that the person that supplied the illegal drugs was **SAULTZ** and that **SAULTZ** and **WASHINGTON** are at the top of the DTO for supplying narcotics with **PRICE** directly

underneath them in the hierarchy. **BURRIS** indicated that she sometimes went inside **SAULTZ's** residence to get the narcotics and that the drug packages usually consisted of crack-cocaine, fentanyl, Xanax, and crystal meth. **BURRIS** stated she took the narcotics to **PRICE**, but that **PRICE** would also keep his own narcotics from **SAULTZ**. **BURRIS** also stated that **BOURDO** would force some of the prostitutes who do not have active warrants to carry packages of drugs from **SAULTZ's** residence on behalf of the DTO.

30. On May 17, 2022, a federal court order for the interception of wire and electronic communications for three separate telephone lines being utilized by Cordell **WASHINGTON** was obtained as it related to the investigation into this DTO and their illegal activities. On June 17, 2022, that federal court order was renewed for the continued wire and electronic interceptions of the telephone lines associated to **WASHINGTON**.
31. On June 9, 2022, a federal court order for the interception of wire and electronic communications for the telephone line being utilized by Patrick **SAULTZ** was obtained as it related to the investigation into this DTO and their illegal activities.
32. Based on the information obtained in the wire and electronic communications, in conjunction with the history of the investigation and the physical and electronic surveillance of this DTO, between June 29, 2022, and July 1, 2022, law enforcement executed ten search warrants on residences and storage facilities and four search warrants on vehicles related to the DTO led by **WASHINGTON** and **SAULTZ**. The searches of those locations, which included the location of **SAULTZ's** residence at 140 Whitethorne Avenue, Columbus, Ohio, led to the seizure of over \$1,000,000 in U.S. currency, copious amounts of suspected narcotics, and over 40 firearms.
33. More specifically, on June 28, 2022, your affiant obtained a search warrant for the residence of 140 Whitethorne Avenue in Columbus, Ohio. This was the primary residence of Patrick **SAULTZ** who investigators have identified as one of the leaders of this DTO.
34. On June 29, 2022, search warrants were executed at the residences of 140 Whitethorne Avenue in Columbus, Ohio; 559 South Burgess Avenue in Columbus, Ohio; 150 Balderson Drive in Pickerington, Ohio; 430 A South Warren Avenue in Columbus, Ohio; 430 B South Warren Avenue in Columbus, Ohio; 505 South Harris Avenue in Columbus, Ohio; and 139 South Princeton Avenue in Columbus, Ohio. During the execution of the search warrants,

the following individuals were arrested pursuant federal criminal complaints: **SAULTZ**, **WASHINGTON**, **PRICE**, **BOURDO**, Tavarryan **JOHNSON**, **ALLISON**, and Alexis **LEWIS**.

35. The search warrant execution at 140 Whitethorne yielded the recovery of crack cocaine and drug paraphernalia. In addition, a number of other items of evidentiary value were recovered, including but not limited to a pistol, approximately \$95,577 in U.S. currency, a suspected drug ledger, and lottery tickets. Investigators know this DTO to distribute drugs in lottery tickets. **SAULTZ** and **LEWIS** were encountered during the execution of the search warrant and arrested pursuant to federal arrest warrants in conjunction with the federal criminal complaints. Numerous cell phones were recovered at the residence of 140 Whitethorne Avenue and in **SAULTZ**' BMW, which are outlined in **Attachment A**. All of those devices were subsequently transported to the Columbus Division of Police property room and have remained in law enforcement custody since the time they were seized.
36. On June 30, 2022, the Grand Jury returned an indictment for numerous **TARGET SUBJECTS** related to this DTO, to include **WASHINGTON**, **SAULTZ**, **ALLISON**, **PRICE**, **BOURDO**, **LEWIS**, and **JOHNSON**, who were charged with federal offenses related to drug trafficking and conspiracy to commit the like.
37. I am aware, through training and experience, that it is common for narcotics traffickers to utilize multiple cellular phones as well as multiple cell phone numbers to arrange and complete narcotics transactions. I am also aware, through training and experience, that it is common for narcotics traffickers to utilize multiple cellular phones as well as multiple cell phone numbers to contact their customer base as well as sources of supplies to obtain the narcotics in which they traffic.
38. Your affiant believes information and evidence related to the DTO, and specifically the **TARGET SUBJECTS**, including **WASHINGTON** and **SAULTZ**, will be recovered from the **SUBJECT DEVICES**. Your affiant would again note that **SAULTZ** was identified as a leader of this DTO. Based upon the above information that has been gathered to date by your affiant, as well as your affiant's knowledge that phones are routinely used to plan, coordinate, and facilitate narcotics transactions, your affiant believes that there is probable cause that the **SUBJECT DEVICES** contains additional evidence of the **TARGET**

OFFENSES as it relates to the operation of and members of this DTO including, but not limited to, **WASHINGTON** and **SAULTZ**.

SEARCH METHODOLOGY TO BE EMPLOYED

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:
- A. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
 - B. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
 - C. Surveying various files, directories and the individual files they contain;
 - D. Opening files in order to determine their contents;
 - E. Scanning storage areas;
 - F. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
 - G. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.
40. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

AUTHORIZATION REQUEST

41. Based on all the forgoing factual information, there is probable cause to believe that violations of violations of A) the distribution and possession with intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); (B) the use of a communications facility in the commission of controlled substances offenses, in violation of Title 21, United States Code, Section 843(b); (C) attempts and conspiracies to commit the aforementioned crimes, in violation of Title 21, United States Code, Section 846; (D) money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957; (E) aiding and abetting the aforementioned crimes, in violation of Title 18, United States Code, Section 2; (F) sex trafficking by means of force, threats, fraud, or coercion, in violation of Title 18, United States Code, Sections 1591(a); and (G) obstruction or conspiracy to commit sex trafficking, in violation of Title 18, United States Code, Section 1591(d) and 1594, have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the **SUBJECT DEVICES** listed in **Attachment A**, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT DEVICES** described in **Attachment A**, and the seizure of the items described in **Attachment B**.

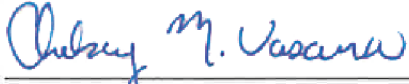
REQUEST FOR SEALING

42. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.



Trace Way
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 7th day of September, 2022.



Chelsey M. Vascara
United States Magistrate Judge
Southern District of Ohio

ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEARCHED

Items Seized From 140 Whitethorne Avenue

1. Purple Samsung phone, IMEI 351782461239384, in the east bedroom on the bedside table
2. White iPhone, IMEI 353096104435798, in living room on couch
3. Black iPhone in clear case, in living room on the couch
4. Red-backed iPhone with white face in clear case, on living room table
5. Pink-backed iPhone with white face in Off-White case, on living room table
6. Pink-backed iPhone with "S" in a square with white face in black case, on living room table
7. Blue Samsung phone in green-and-brown case, IMEI 358688105639041, on living room table

Items Seized From SAULTZ'S BMW at 140 Whitethorne Avenue

1. Black Samsung phone in black case, IMEI 350345701290897, in the driver's door

This warrant authorizes the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of A) the distribution and possession with intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); (B) the use of a communications facility in the commission of controlled substances offenses, in violation of Title 21, United States Code, Section 843(b); (C) attempts and conspiracies to commit the aforementioned crimes, in violation of Title 21, United States Code, Section 846; (D) money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957; (E) aiding and abetting the aforementioned crimes, in violation of Title 18, United States Code, Section 2; (F) sex trafficking by means of force, threats, fraud, or coercion, in violation of Title 18, United States Code, Sections 1591(a); and (G) obstruction or conspiracy to commit sex trafficking, in violation of Title 18, United States Code, Section 1591(d) and 1594; (hereinafter collectively referred to as the **TARGET OFFENSES**), including but not limited too:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. List of customers and related identifying information;
3. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
4. Any information related to source of drugs (including names, addresses, phone numbers, or any other identifying information);
5. Any information related to travel or schedule, particularly for the purpose of obtaining quantities of narcotic drugs;
6. All locations information pertaining to the transportation and storage of narcotics and narcotics proceeds and accompanying locations including residences, storage units, and financial institutions;
7. All bank records, checks, credit card bills, account information, and other financial records;

8. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
9. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs, and electronic messages,) pertaining to the **TARGET OFFENSES**.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service, including any social media accounts.
11. Any and all messages, emails, voicemails, texting applications, text messaging, or social media communications pertaining to prostitution or sex trafficking, including, but not limited to, hotel/motel reservations, car services, posting of prostitution advertisements, and communications regarding the scheduling of dates or payment for sexual services.
12. Any and all lists of names, telephone numbers, and addresses related to the operation of sex trafficking/prostitution services and drug trafficking.
13. Any and all records, files, or documents showing dominion, ownership, custody, or control over the **SUBJECT DEVICE** including evidence showing user attrition at the time the things described in the warrant were created, edited, deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.